IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Valerie FAVIER ET AL.

Serial No.: 09/740,801

Filed: December 21, 2000

For: METHOD AND DEVICE FOR CONFIGURING A FIREWALL IN A COMPUTER SYSTEM

Examiner:

Group Art Unit:

Corres. To FR 99/16118
Filed December 21, 1999

McLean, Virginia

COMPLETION OF
CLAIM FOR BENEFIT OF FILING DATE
OF PRIOR FOREIGN APPLICATION

Honorable Commissioner of Patents and Trademarks
Washington, DC 20231

Sir:

Further to the Claim for Priority filed with the application on December 21, 2000, in the matter of the above-identified application, a claim is hereby made under the provisions of 35 U.S.C. §119 for the benefit of the filing date of the corresponding French application No. 99 16118 filed December 21, 1999, which is referred to in the Declaration of the present case.

A certified copy of said French application is attached.

Respectfully submitted,

Miles & Stockbridge P.C.

Date March 23, 2001

By: Edward J. Kondracki

Edward J. Kondracki
Registration No. 20,604

Miles & Stockbridge, P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Tel.: (703) 903-9000

R E P U B L I Q U E F R A N Ç A I S E

BULL S.A.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 27 DEC. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire — D3 540 W /250899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 21 DEC 1999
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 9916118

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 21 DEC 1999

Vos références pour ce dossier *(facultatif)* FR 3845/PB

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

BULL S.A.
BERTRANDIAS Patricia - PC/58D20
68, route de Versailles

78434 LOUVECIENNES Cedex

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE ET DISPOSITIF DE CONFIGURATION DE PARE-FEU DANS UN SYSTEME INFORMATIQUE.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		BULL S.A.
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		6 4 2 0 5 8 7 3 9
Code APE-NAF		3 0 0 C
Adresse	Rue	68, route de Versailles
	Code postal et ville	78430 LOUVECIENNES
Pays		France
Nationalité		Française
N° de téléphone *(facultatif)*		01.39.66.66.34
N° de télécopie *(facultatif)*		01.39.66.61.73
Adresse électronique *(facultatif)*		PATRICIA.BERTRANDIAS@BULL.NET

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 21 DEC 1999
75 INPI PARIS
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 9916118

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		FR 3845/PB
6 MANDATAIRE		
Nom		BERTRANDIAS
Prénom		Patricia
Cabinet ou Société		BULL S.A.
N °de pouvoir permanent et/ou de lien contractuel		PG 4972
Adresse	Rue	68, route de Versailles / PC 58D20
	Code postal et ville	78434 LOUVECIENNES CEDEX
N° de téléphone *(facultatif)*		01.39.66.66.34
N° de télécopie *(facultatif)*		01.39.66.61.73
Adresse électronique *(facultatif)*		PATRICIA.BERTRANDIAS@BULL.NET
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		0

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

Patricia BERTRANDIAS
(Salarié BULL S.A)

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1/1

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier *(facultatif)*	**FR 3845/PB**
N° D'ENREGISTREMENT NATIONAL	9916118

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE ET DISPOSITIF DE CONFIGURATION DE PARE-FEU DANS UN SYSTEME INFORMATIQUE.

LE(S) DEMANDEUR(S) :

BULL S.A.
68, route de Versailles
78430 LOUVECIENNES - FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		**Favier**
Prénoms		**Valérie**
Adresse	Rue	La Croix de Pinet
	Code postal et ville	38410 ST MARTIN DE L'URIAGE - FRANCE
Société d'appartenance *(facultatif)*		
Nom		**Guionneau**
Prénoms		**Christophe**
Adresse	Rue	198 Cours de la Libération
	Code postal et ville	38100 GRENOBLE - FRANCE
Société d'appartenance *(facultatif)*		
Nom		**Grardel**
Prénoms		**Frédéric**
Adresse	Rue	9 rue Casimir Brenier
	Code postal et ville	38120 ST EGREVE - FRANCE
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

Louveciennes, le 17 décembre 1999

BERTRANDIAS Patricia (Salarié Bull S.A.)

PROCEDE ET DISPOSITIF DE CONFIGURATION DE PARE-FEU DANS UN SYSTEME INFORMATIQUE

La présente invention concerne le domaine de pare-feu dans un système informatique, et plus particulièrement de la configuration de pare-feu.

L'art antérieur

Un pare-feu est une machine ou groupes de machines permettant de sécuriser la jonction entre un réseau intérieur et un réseau extérieur tel qu'Internet contre des intrusions non autorisées, voire malveillantes. Il est rappelé qu'Internet consiste en un ensemble de réseaux et machines interconnectés dans le monde entier, permettant à des utilisateurs des quatre coins de la terre de partager des informations.

Le terme « machine » dans la présente description représente une unité conceptuelle très large, de nature matériel et/ou logiciel. Les machines peuvent être très diverses, telles que des stations de travail, serveurs, routeurs, machines spécialisées et passerelles entre réseaux.

Tous les messages transitant entre le réseau intérieur et extérieur doivent passer par le pare-feu qui examine chaque message et bloque ceux qui ne répondent pas à des règles de contrôle d'accès déterminées. Le pare-feu est un élément d'une politique globale de sécurité, intégré dans un environnement applicatif de plus en plus riche et destiné à protéger des ressources d'information.

Les pare-feux sont utilisés notamment pour empêcher les utilisateurs d'Internet non autorisés d'accéder à des réseaux internes connectés à Internet, pour donner à un utilisateur d'un réseau interne l'accès à Internet

de manière sûre, pour séparer les machines publiques d'une entreprise permettant l'accès à Internet de son réseau interne, pour réaliser un cloisonnement à l'intérieur d'un réseau donné, pour protéger les segments de réseaux internes cloisonnés.

Le pare-feu est matérialisé par exemple par une machine dédiée qui contrôle l'accès aux différentes machines d'un réseau intérieur déterminé.

Pour ce faire, le pare-feu contrôle quelles machines et/ou quels utilisateurs et/ou quels services ou applications d'un réseau intérieur peuvent accéder à quelle machine et/ou quels utilisateurs et/ou quels services ou applications d'un réseau extérieur et inversement.

Les machines appartenant au réseau Internet utilisent le protocole TCP/IP. Le pare-feu effectue des filtrages des communications TCP/IP. Le pare-feu manipule des données applicatives, informations transmises dans la partie réservée aux données dans les en-têtes des datagrammes TCP/IP.

Les critères de filtrage sont par exemple de manière non limitative :

- l'adresse appelante,
- l'adresse appelée,
- l'application appelée.

La complexité de configuration de pare-feu est illustrée par l'exemple suivant, auquel peuvent être ramenées la plupart des architectures de cloisonnement dans les réseaux d'entreprises.

On considère le cas d'un réseau d'entreprise comprenant n pare-feu dénommés NW_1, ..., NW_n connectés à des sous-réseaux.

On souhaite appliquer une politique de sécurité selon laquelle sur chaque sous-réseau CC_i, une station de travail (poste client) C_i est autorisée à accéder à un serveur S_i situé sur un sous-réseau SS_i. Les sous-réseaux CC_i et SS_i sont reliés à un unique et même pare-feu NW_i.

Ce cas de figure peut bien évidemment être étendu au cas de plusieurs stations de travail, autorisées à accéder à plusieurs serveurs.

Avec les systèmes de configuration de pare-feu classiques, les administrateurs opèrent de deux manières :

- Définir deux groupes contenant respectivement les stations de travail et les serveurs. Définir ensuite une règle autorisant l'accès du groupe des stations de travail vers le groupe des serveurs. Cette manière de procéder permet d'autoriser en une seule règle l'accès de chaque station au serveur connecté au même pare-feu (C_i -> S_i), mais autorise également l'accès des stations à tous les autres serveurs connectés à d'autres pare-feu NW_j (C_i -> S_j). Ce n'est pas la politique de sécurité souhaitée.
- Définir sur chaque pare-feu les règles spécifiques autorisant un à un les accès de chaque station de travail au serveur qui lui correspond. Cette manière de procéder est très vite fastidieuse, voire difficile à mettre en pratique, lorsque le nombre de pare-feu augmente, voire le nombre de stations, ou le nombre de serveurs.

La simplification de la configuration est un objectif prioritaire d'un administrateur de pare-feu.

Les solutions courantes connues pour tenter de résoudre le problème de complexité de configuration sont les suivantes.

On connaît un système commercialisé sous l'appellation Net Partitioner et produit par la Société Solsoft.

Le dispositif Net Partitioner permet à l'administrateur de représenter graphiquement l'ensemble de son réseau, avec l'implantation des pare-feu, ainsi que des différents serveurs et des stations de travail qui en font partie. Les machines sont représentées par des icônes et leur interconnexion par des traits les reliant.

L'administrateur définit également sous forme de flèches la manière dont les machines peuvent accéder à d'autres machines et aux applications qu'elles hébergent.

Cette solution permet de définir des groupes d'ordinateurs, ainsi que des règles de contrôle d'accès entre ces groupes. En revanche, les règles définissent l'accès de tous les éléments d'un groupe vers tous les éléments d'un autre groupe, ce qui alourdit la procédure de configuration.

La description du système (à savoir l'ensemble des machines présentes sous forme d'icônes et leur interconnexion sous forme de traits) et la spécification des règles appliquées au système et représentées sous forme de flèches sont combinées sur une même interface graphique. Plus le système comprend de machines et plus les connexions entre ces machines sont nombreuses, plus il est difficile pour l'administrateur de décrire le système à partir de l'interface.

Par ailleurs, le dispositif Net Partitioner ne prévoit aucun transfert des règles depuis ledit dispositif vers les pare-feu concernés et aucune prise en compte de la nouvelle politique de sécurité. L'administrateur doit lui-même configurer chacun des pare-feu à partir des résultats procurés par le dispositif Net Partitioner.

Cette solution ne permet donc pas de simplifier la procédure de configuration.

Un but de la présente invention est de simplifier la configuration d'un grand nombre de pare-feu.

Résumé de l'invention

Dans ce contexte, la présente invention propose un procédé de configuration de pare-feu dans un système informatique comportant des objets, les objets pour lesquels une politique de contrôle d'accès est mise en place étant appelés des ressources, caractérisé en ce qu'il regroupe les objets du système par domaine de protection, chaque pare-feu assurant la protection d'un domaine intérieur par rapport à un domaine extérieur et applique au pare-feu concerné une règle de contrôle d'accès entre une ressource d'origine et une ressource de destination uniquement si lesdites ressources d'origine et de destination appartiennent au même domaine ou de protection.

La présente invention concerne également le système de mise en œuvre dudit procédé.

Présentation des figures

D'autres caractéristiques et avantages de l'invention apparaîtront à la lumière de la description qui suit, donnée à titre d'exemple illustratif et non limitatif de la présente invention, en référence aux dessins annexés dans lesquels:

- la figure 1 est une vue schématique du système selon une forme de réalisation de l'invention ;

•la figure 2 est une copie d'écran d'une interface graphique présentant des pare-feu du système selon la figure 1 et à leurs propriétés ;

•la figure 3 est une copie d'écran d'une interface graphique présentant des groupes de machines du système selon la figure 1 ;

•la figure 4 est une copie d'écran d'une interface graphique présentant des règles de contrôle d'accès dans le système selon la figure 1.

Description d'une forme de réalisation de l'invention

Comme le montrent les figures 1 à 4, la présente invention se rapporte à un procédé de configuration de pare-feu 1 dans un système informatique 2.

Le système informatique 2 est distribué et comprend des objets 3, des utilisateurs et les pare-feu 1. Un objet 3 est une unité conceptuelle très large, de nature matérielle et/ou logicielle. Les objets 3 peuvent être très divers, tels que des réseaux, des sous-réseaux, des stations de travail, des serveurs, des routeurs, des machines spécialisées et passerelles entre réseaux, des applications. Seuls les composants des objets 3 du système 2 caractéristiques de la présente invention seront décrits, les autres composants étant connus de l'homme du métier. Les objets 3 entre lesquels des règles de contrôle d'accès constituant la politique de sécurité du système 2 sont définies, sont appelés ressources 4.

Comme représenté sur la figure 1, les pare-feu 1 assurent la protection d'un domaine intérieur 5 (D1, D2, D3) par rapport à un domaine extérieur 6 (dorsal, en anglais backbone). Un administrateur 7 définit pour chaque pare-feu 1 le domaine intérieur 5 constituant le domaine de protection du pare-feu. Le domaine de protection du pare-feu représente ce que l'administrateur souhaite protéger à l'aide dudit pare-feu par rapport à ce dont il veut le protéger, à savoir le domaine extérieur.

Chacun des deux domaines de protection 5 et extérieur 6 est constitué de zones 8 comportant un ou plusieurs réseaux ou sous-réseaux 9 de machines. Une zone 8 est une partie du système 2 séparé du reste de celui-ci par un ou plusieurs pare-feu. Les zones 8 sont connectées au pare-feu 1 concerné par plusieurs interfaces réseaux 10. L'administrateur 7 détermine pour chaque zone 8 raccordée à chaque pare-feu, si la zone 8 est à l'intérieur du domaine 5 de protection du pare-feu (zone intérieure) ou si elle est à l'extérieur (zone extérieure), c'est à dire si elle est directement protégée par le pare-feu ou s'il s'agit d'une zone assurant la liaison entre les pare-feu, ou ce qui est équivalent, entre les différents domaines de protection.

Dans l'exemple de forme de réalisation illustré sur la figure 1, chaque domaine 5 de protection, D1, D2, D3 est contrôlé par un pare-feu 1 respectivement NW1, NW2, NW3. Chacun des pare-feu NW1, NW2, NW3 est connecté à une zone 8 comprenant un sous-réseau 11 interne respectivement I_1, I_2, I_3 et à une zone 8 comportant un sous-réseau 12 de type « zone démilitarisée » respectivement DMZ_1, DMZ_2, DMZ_3. Les sous-réseaux 11 et 12 sont à l'intérieur du domaine 5 de protection.

Un sous-réseau de type « zone démilitarisée » est un sous-réseau tampon, réalisant une sorte de sas entre un réseau interne et externe pour en renforcer la protection.

Chaque pare-feu 1 est relié à une zone 8 du domaine 6 extérieur, comportant un réseau 13 dit réseau dorsal. La zone 8 du domaine 6 extérieur comprenant le réseau 13 est appelée zone dorsale. La zone 8 dorsale constitue la liaison du domaine intérieur 5 avec le reste du réseau concerné, et représente l'extérieur par rapport au domaine 5 considéré.

Selon un développement de l'invention, la zone 8 dorsale comprend une machine 14 de configuration centrale à partir de laquelle la configuration globale du système 2 est effectuée. La configuration globale du système 2 peut être réalisée par exemple de la manière explicitée dans la demande de brevet déposée par le présent déposant le même jour que la présente demande et dont le titre est « Procédé et dispositif de configuration centralisée de pare-feu dans un système informatique ». La machine 14 de configuration centrale offre une interface 15 graphique permettant à l'administrateur 7 de réaliser ladite configuration. L'interface 15 graphique est illustrée sur les figures 1 à 4.

La présente invention est décrite dans ce qui suit dans la forme de réalisation du système illustré sur les figures 1 à 4 consistant en une configuration centrale des pare-feu. Le procédé selon l'invention décrit pour ladite forme de réalisation est susceptible d'être appliqué à un pare-feu isolé sans configuration centrale.

Dans la forme de réalisation illustré sur la figure 2, l'administrateur saisit la définition des pare-feu 1, des domaines 5, 6 et des interfaces réseaux 10 au travers de l'interface 15 graphique. L'écran de l'interface 15 est divisé en trois fenêtres : une fenêtre 16 d'objets à gauche de l'écran de la machine 14, une fenêtre 17 d'attributs à droite de l'écran de la machine 14., une fenêtre 18 de règles en bas de l'écran. Dans la fenêtre 16 d'objets, lorsqu'un onglet 19 « Netwalls » est sélectionné, tous les pare-feu NW1, NW2, NW3 du système 2 sont indiqués. Dans la fenêtre 17 d'attributs, lorsqu'un onglet 20 « Properties » est sélectionné, les propriétés du pare-feu surligné dans la partie gauche (ici NW1) sont précisées dans un tableau 21 de zones.

L'administrateur définit les propriétés des pare-feu 1 de la manière suivante. Le pare-feu NW1 dispose de trois interfaces réseaux 10

mentionnées dans la colonne 22 « Name » avec des zones 8 indiquées dans la colonne 23 « Zone » : une interface réseau NW1 avec la zone du sous-réseau I1, une interface réseau NW1_dmz avec la zone du sous-réseau DMZ_1 et une interface réseau NW1_dorsale avec la zone dorsale. Les propriétés sont similaires pour les pare-feu NW_2 et NW_3. Une colonne 24 « Address » du tableau 21 indique les adresses des interfaces réseau, dont la désignation est située sur la même ligne.

Une colonne 25 « Is External » du tableau 21 de zones permet de spécifier pour chaque interface réseau 10 si ladite interface réseau est attachée à une zone 8 extérieure au domaine 5 de protection (valeur « true ») ou intérieure au domaine de protection (valeur « false »).

Dans l'exemple considéré, les interfaces réseaux NW1_dmz et NW1 sont attachées à des zones 8 intérieures (sous-réseaux DMZ_1, I_1) au domaine 5 de protection, alors que l'interface réseau NW1_dorsale est extérieure (réseau dorsal) au domaine de protection (configuration similaire pour les pare-feu NW_2 et NW_3).

Chaque pare-feu assure les contrôles d'accès à la fois des communications entre les domaines 5 et des communications entre les zones 8 à l'intérieur du domaine 5 dont il est responsable. Une partie de la politique de sécurité concerne le contrôle des accès entre les domaines ; une autre partie de la politique de sécurité concerne le contrôle des accès entre des zones à l'intérieur du domaine de contrôle du pare-feu.

L'invention consiste à définir une opération de factorisation des règles de contrôle d'accès constituant la politique de contrôle d'accès dans le but de minimiser le nombre de règles de filtrage à déclarer par l'administrateur.

Pour ce faire, l'administrateur 7 réunit au sein de mêmes groupes les objets 3 du système 2 (dans l'exemple illustré, des stations de travail et serveurs) pour lesquels une même politique de sécurité est appliquée. Dans l'exemple illustré sur la figure 1, des stations de travail 26 C_1, C_2, C_3 font partie intégrante des sous-réseaux internes respectivement I_1, I_2, I_3 ; des serveurs 27 S_1, S_2, S_3 appartiennent respectivement aux sous-réseaux DMZ_1, DMZ_2, DMZ_3. Le domaine D1 rassemble la zone comprenant le sous-réseau interne I1 avec la station de travail C1 et la zone comprenant le sous-réseau DMZ1 avec le serveur S1. Dans l'exemple illustré, une seule station de travail appartient au sous-réseau interne I1 : le sous-réseau I1 aurait pu contenir plusieurs stations de travail, C11, C12, C13, ..., C1k et/ou tout autre type de machines. De même, le sous-réseau DMZ1 aurait pu contenir plusieurs serveurs, S11, S12, S13, ..., S1m et/ou tout autre type de machines. Le même raisonnement est applicable aux autres domaines et zones.

L'administrateur 7 peut, à titre illustratif, réunir dans un groupe de stations de travail 26 les machines C_1, C_2, C_3 et dans un groupe de serveurs 27 les machines S_1, S_2, S_3.

L'invention consiste à déclarer entre les types de groupes définis par l'administrateur des règles de contrôle d'accès de portée limitée à chaque pare-feu ou étendue au système 2. L'administrateur spécifie pour les règles de contrôle d'accès, si la portée est locale au pare-feu ou globale.

Une règle de portée locale définit des relations d'accès entre des ressources 4 de deux groupes, lesdites ressources appartenant à un même domaine 5 de protection. La portée locale permet de restreindre la règle à des accès intérieurs au domaine 5 de protection.

Dans l'exemple mentionné plus haut, une règle de portée locale définit une relation d'accès du groupe (C_1, ..., C_n) vers le groupe (S_1, ..., S_n) en mettant en jeu un accès depuis la ressource C_i vers la ressource S_i, sans établir de relation de C_i vers S_j, avec j différent de i. Dans le cas de plusieurs stations de travail et serveurs comme vu plus haut, le principe est le même : la règle de portée locale définit une relation d'accès du groupe (C_{11},C_{12}, ..., C_{1K} ..., C_{n1}, C_{n2}...) vers le groupe (S_{11},S_{12}, ..., S_{1m}, ..., S_{n1}, S_{n2}...) en mettant en jeu un accès depuis la ressource C_{ik} vers la ressource S_{im}, sans établir de relation de C_{ik} vers S_{jm}, avec j différent de i et quelque soit k et m.

Une règle de portée globale définit les relations d'accès possibles entre deux groupes dans le système 2 dans son entier.

Une règle de portée globale est conservée et toujours utilisable par l'administrateur pour traiter les cas généraux de la politique de sécurité. Les règles de portée globale régissent les relations d'accès du groupe (C_1, ..., C_n) vers le groupe (S_1, ..., S_n) et établissent toutes les relations de C_i vers S_j, pour i et j variant de 1 à n. Dans le cas de plusieurs stations de travail et serveurs comme vu plus haut, la règle de portée globale définit une relation d'accès du groupe (C_{11},C_{12}, ..., C_{1K} ..., C_{n1}, C_{n2}...) vers le groupe (S_{11},S_{12}, ..., S_{1m}, ..., S_{n1}, S_{n2}...) en mettant en jeu un accès depuis la ressource C_{ik} vers la ressource S_{im}, quelque soit i, j, k et m.

L'attribut de portée « locale » ou « globale » de chaque règle est attaché à chaque règle, de telle manière que chaque pare-feu a individuellement la connaissance de la portée des règles.

Dans la forme de réalisation illustrée sur les figures 3 et 4, l'administrateur souhaite mettre en œuvre une politique de contrôle d'accès selon laquelle les ressources de chaque sous-réseau interne I_i (i variant ici de 1 à 3) de chaque domaine 5 de protection peuvent accéder aux

ressources du sous-réseau DMZ_i (i variant ici de 1 à 3) du même domaine 5 de protection, sans autoriser l'accès entre un sous-réseau I_i interne d'un domaine donné et le sous-réseau DMZ_j, avec j différent de i, d'un autre domaine (par exemple, accès entre le sous-réseau I_1 et le sous-réseau DMZ_2).

Comme le montre la figure 3, l'administrateur regroupe à l'aide de l'interface 15 graphique les zones des sous-réseaux internes I_1, I_2, I_3 dans le groupe des sous-réseaux internes G_I et les zones des sous-réseaux DMZ_1, DMZ_2, DMZ_3 dans le groupe G_DMZ. Dans la fenêtre 16 d'objets, un onglet 28 « Ressources » étant sélectionné, il est indiqué que le groupe G_DMZ comprend ANY_DMZ_1, ANY_DMZ_2, ANY_DMZ_3, à savoir l'ensemble des objets des sous-réseaux DMZ_1, DMZ_2, DMZ_3.

L'administrateur définit ensuite dans la fenêtre 18 de règles les règles de portée locale ou globale. Dans l'exemple illustré sur la figure 4, un tableau 29 de règles dans la fenêtre 18 de règles permettant de définir les règles est affiché dans la fenêtre 17 d'attributs lorsqu'un onglet 30 « Rules » est sélectionné. La fenêtre 17 d'attributs montre que l'administrateur a défini à l'aide du tableau 29 de la fenêtre 18 une règle de portée « locale » autorisant l'accès depuis le groupe G_I vers le groupe G_DMZ, la règle ainsi définie étant affichée dans le tableau 29 de la fenêtre 17 d'attributs.

Le tableau 29 de règles comprend une colonne 31 « Name » pour identifier la règle de contrôle d'accès, une colonne 32 « Source » pour désigner le groupe d'origine de la règle, une colonne 33 « Destination » pour désigner le groupe destination de la règle.

La portée de la règle est définie dans une colonne 34 « Scope » et peut prendre les valeurs « LOCAL » pour une portée locale ou « GLOBAL »

pour une portée globale. Dans l'exemple illustré, la portée de la règle prend la valeur par défaut « GLOBAL ».

Le procédé selon la présente invention opère de la manière suivante :

Au moment où le pare-feu effectue le contrôle d'accès (par exemple lors d'une tentative d'établissement de connexion), le pare-feu 1 analyse l'attribut de portée de la règle régissant le contrôle de l'accès en cours.

Si la règle est de portée globale, elle est appliquée sans contrôle supplémentaire : l'accès est autorisé ou rejeté en fonction de la consigne donnée par la règle. Il s'agit d'un fonctionnement standard de pare-feu.

Si la portée de la règle est locale, le pare-feu détermine les interfaces réseaux 10 d'entrée et de sortie du trafic en cours de traitement et analyse si ces interfaces réseaux sont attachées au domaine 5 intérieur ou 6 extérieur.

Si les deux interfaces réseaux 10 d'entrée et de sortie sont attachées au domaine 5 intérieur, le trafic en cours de traitement reste à l'intérieur du domaine 5 de protection du pare-feu : la règle est alors appliquée et l'accès est autorisé ou rejeté en fonction de la consigne donnée par ladite règle.

Si l'une des deux interfaces réseaux 10 est attachée au domaine 6 extérieur, le trafic en cours de traitement n'est pas interne au domaine 5 de protection du pare-feu : la règle en question n'est pas applicable pour le profil de trafic en cours de traitement.

Dans l'exemple illustré, aucun pare-feu reliant les domaines D1, D2, D3 entre eux n'est prévu. L'invention ne s'intéresse pas aux domaines de liaison. Les interfaces associées aux domaines de liaison sont

automatiquement attachées à un domaine externe, à savoir que la colonne « Is External » prend la valeur true.

Dans l'exemple illustré sur les figures 2 à 5, le procédé opère de la manière suivante.

Lors d'un accès depuis le sous-réseau I_1 vers le sous-réseau DMZ_1, le pare-feu NW_1 détermine que le trafic entre par l'interface réseau 10 NW_1 et ressort par l'interface réseau 10 NW_1_dmz. Lesdites interfaces réseau NW_1 et NW_1_dmz sont déclarées intérieures au domaine de protection du pare-feu en question. Le pare-feu NW_1 autorise l'accès. Le mécanisme est similaire pour des accès du sous-réseau I_2 vers DMZ_2, au travers de NW_2, et de I_3 vers DMZ_3, au travers de NW_3.

Lors d'un accès du sous-réseau I_1 vers le sous-réseau DMZ_2, le pare-feu NW_1 détermine que le trafic entre par l'interface réseau NW_1 et ressort par l'interface réseau NW_1_dorsale. La première interface réseau NW_1 est déclarée intérieure au domaine 5 de protection, alors que la seconde NW_1_dorsale est déclarée extérieure au domaine 5 de protection. Le trafic n'est pas limité au domaine 5 de protection et la pare-feu NW1 n'autorise pas l'accès.

De la même manière, le pare-feu NW_2 détecte que le trafic en cause entre par l'interface réseau NW_2_dorsale et ressort par l'interface réseau NW_2_dmz. L'interface réseau NW_2_dorsale est attachée à un sous-réseau extérieur au domaine de protection ; le trafic n'est pas limité au domaine de protection du pare-feu NW_2 et est bloqué par ce dernier.

La présente invention concerne le procédé de configuration de pare-feu 1 dans un système 2 informatique comportant des objets 3, les objets 3 pour lesquels une politique de contrôle d'accès est mise en place étant

appelés des ressources 4, caractérisé en ce qu'il regroupe les objets 3 du système par domaine 5, 6 de protection, chaque pare-feu 1 assurant la protection d'un domaine intérieur 5 par rapport à un domaine 6 extérieur et applique au pare-feu concerné une règle de contrôle d'accès entre une ressource 4 d'origine et une ressource de destination uniquement si lesdites ressources d'origine et de destination appartiennent au même domaine 5 ou 6 de protection.

Le procédé détermine le domaine de protection des ressources 4 au moyen des interfaces réseau 10 du pare-feu concerné, interfaces par lesquels passent les communications pour parvenir aux dites ressources.

Le procédé définit les zones 8 comportant des réseaux ou sous-réseaux ; il associe les interfaces réseaux 10 des pare-feu auxquels lesdites zones sont connectées à un domaine intérieur ou extérieur ; il détermine les interfaces réseaux 10 d'entrée et de sortie du trafic en cours de traitement ; il analyse si lesdites interfaces réseaux sont attachées à un domaine intérieur ou extérieur ; il applique la règle uniquement si les deux interfaces réseaux sont attachées au même domaine 5 intérieur ce qui correspond au fait que les ressources appartiennent au même domaine de protection.

Le procédé constitue les groupes d'objets 3 pour lesquels la politique de contrôle d'accès est identique et applique la règle entre chacune des ressources d'un groupe d'origine et d'un groupe de destination.

Le procédé caractérise la règle par une portée locale ou globale et il applique la règle aux ressources concernées uniquement si lesdites ressources appartiennent au même domaine 5 ou 6 de protection lorsque la portée de la règle est locale, applique la règle à toutes les ressources concernées lorsque la portée de la règle est globale.

La présente invention concerne également le dispositif permettant la mise en œuvre du procédé décrit ci-dessus.

Le présente invention se rapporte également au dispositif de configuration de pare-feu 1 dans le système 2 informatique caractérisé en ce qu'il comprend la machine 14 de configuration centrale permettant de regrouper les objets 3 du système par domaine de protection, chaque pare-feu 1 assurant la protection d'un domaine intérieur 5 par rapport à un domaine 6 extérieur et d'appliquer au pare-feu concerné une règle de contrôle d'accès entre une ressource 4 d'origine et une ressource de destination uniquement si lesdites ressources d'origine et de destination appartiennent au même domaine 5 ou 6 de protection.

Le dispositif comprend l'interface 15 graphique à partir de laquelle un administrateur 7 est susceptible de saisir les domaines 5 et 6 de protection et les règles de contrôle d'accès.

L'interface graphique permet à l'administrateur 7 de définir une portée à la règle de contrôle d'accès locale ou globale, et la machine 14 applique la règle aux ressources concernées uniquement si lesdites ressources appartiennent au même domaine 5 ou 6 de protection lorsque la portée de la règle est locale, et applique la règle à toutes les ressources concernées lorsque la portée de la règle est globale.

REVENDICATIONS

1. Procédé de configuration de pare-feu (1) dans un système (2) informatique comportant des objets (3), les objets (3) pour lesquels une politique de contrôle d'accès est mise en place étant appelés des ressources (4), caractérisé en ce qu'il regroupe les objets (3) du système par domaine (5, 6) de protection, chaque pare-feu (1) assurant la protection d'un domaine intérieur (5) par rapport à un domaine (6) extérieur et applique au pare-feu concerné une règle de contrôle d'accès entre une ressource (4) d'origine et une ressource de destination uniquement si lesdites ressources d'origine et de destination appartiennent au même domaine (5) ou (6) de protection.

2. Procédé selon la revendication 1, caractérisé en ce qu'il détermine le domaine de protection des ressources (4) au moyen des interfaces réseau (10) du pare-feu concerné, interfaces par lesquels passent les communications pour parvenir aux dites ressources.

3. Procédé selon la revendication 2, caractérisé en ce qu'il définit des zones (8) comportant des réseaux ou sous-réseaux, en ce qu'il associe les interfaces réseaux (10) des pare-feu auxquels lesdites zones sont connectées à un domaine intérieur ou extérieur, en ce qu'il détermine les interfaces réseaux (10) d'entrée et de sortie du trafic en cours de traitement, en ce qu'il analyse si lesdites interfaces réseaux sont attachées à un domaine intérieur ou extérieur, et en ce qu'il applique la règle uniquement si les deux interfaces réseaux sont attachées au même domaine (5) intérieur ce qui correspond au fait que les ressources appartiennent au même domaine de protection.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce qu'il constitue des groupes d'objets (3) pour lesquels la politique de contrôle d'accès est identique et applique la règle entre chacune des ressources d'un groupe d'origine et d'un groupe de destination.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce qu'il caractérise la règle par une portée locale ou globale, en ce qu'il applique la règle aux ressources concernées uniquement si lesdites ressources appartiennent au même domaine (5) ou (6) de protection lorsque la portée de la règle est locale, et en ce qu'il applique la règle à toutes les ressources concernées lorsque la portée de la règle est globale.

6. Dispositif permettant la mise en œuvre du procédé selon l'une des revendications 1 à 5.

7. Dispositif de configuration de pare-feu (1) dans un système (2) informatique comportant des objets (3), les objets (3) pour lesquels une politique de contrôle d'accès est mise en place étant appelés des ressources (4), caractérisé en ce qu'il comprend une machine (14) de configuration centrale permettant de regrouper les objets (3) du système par domaine de protection, chaque pare-feu (1) assurant la protection d'un domaine intérieur (5) par rapport à un domaine (6) extérieur et d'appliquer au pare-feu concerné une règle de contrôle d'accès entre une ressource (4) d'origine et une ressource de destination uniquement si lesdites ressources d'origine et de destination appartiennent au même domaine (5) ou (6) de protection.

8. Dispositif selon la revendication 7, caractérisé en ce qu'il comprend une interface (15) graphique à partir de laquelle un administrateur (7) est susceptible de saisir les domaines (5) et (6) de protection et les règles de contrôle d'accès.

9. Dispositif selon l'une des revendications 7 ou 8, caractérisé en ce l'interface graphique permet à l'administrateur (7) de définir une portée à la règle de contrôle d'accès locale ou globale, et en ce que la machine (14) applique la règle aux ressources concernées uniquement si lesdites ressources appartiennent au même domaine (5) ou (6) de protection lorsque la portée de la règle est locale, et applique la règle à toutes les ressources concernées lorsque la portée de la règle est globale.

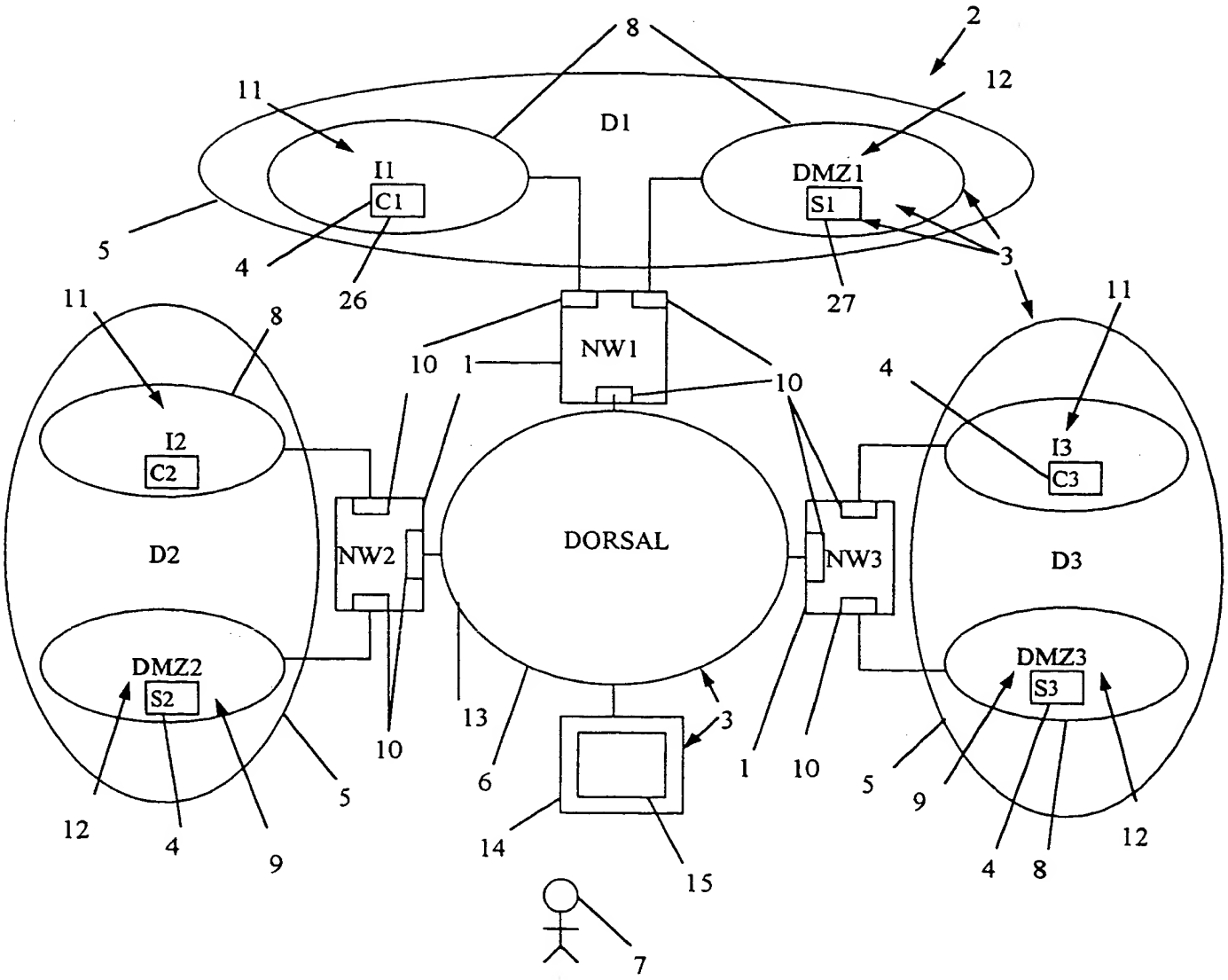
D1
I1
C1
DMZ1
S1
NW1
D2
I2
C2
NW2
DORSAL
NW3
D3
I3
C3
DMZ2
S2
DMZ3
S3
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
26
27

FIG.1

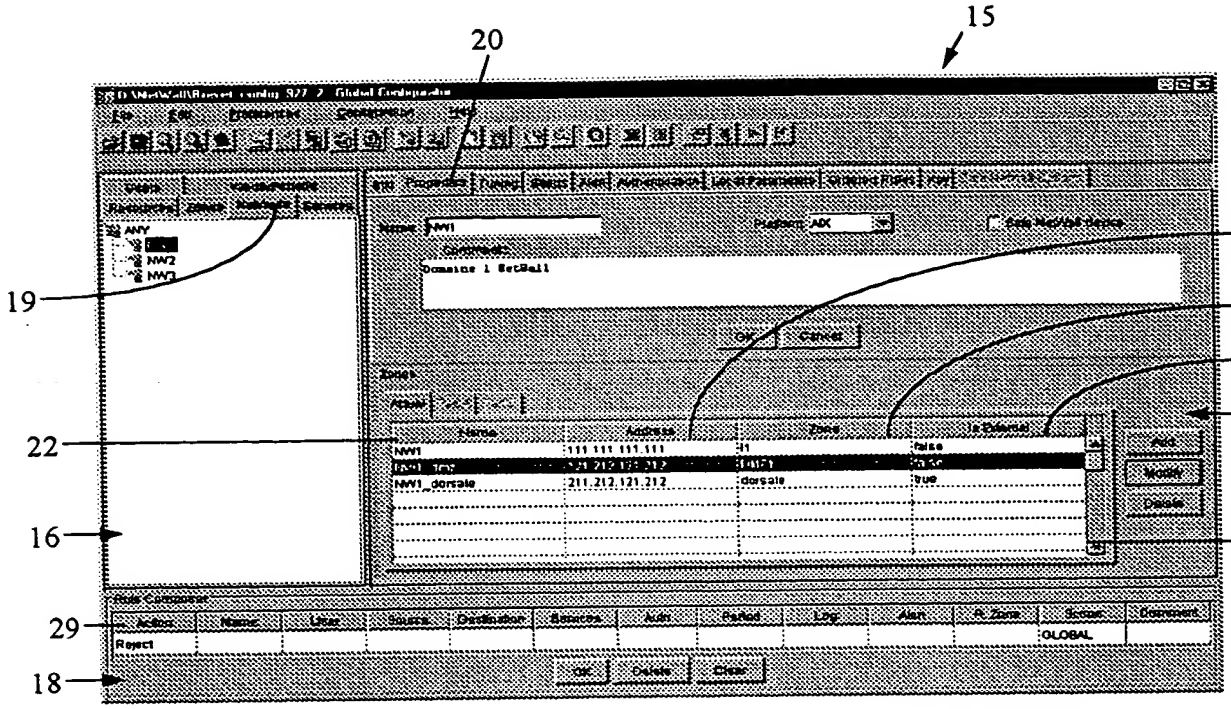
15
20
19
24
23
25
17
22
16
21
29
18

FIG.2

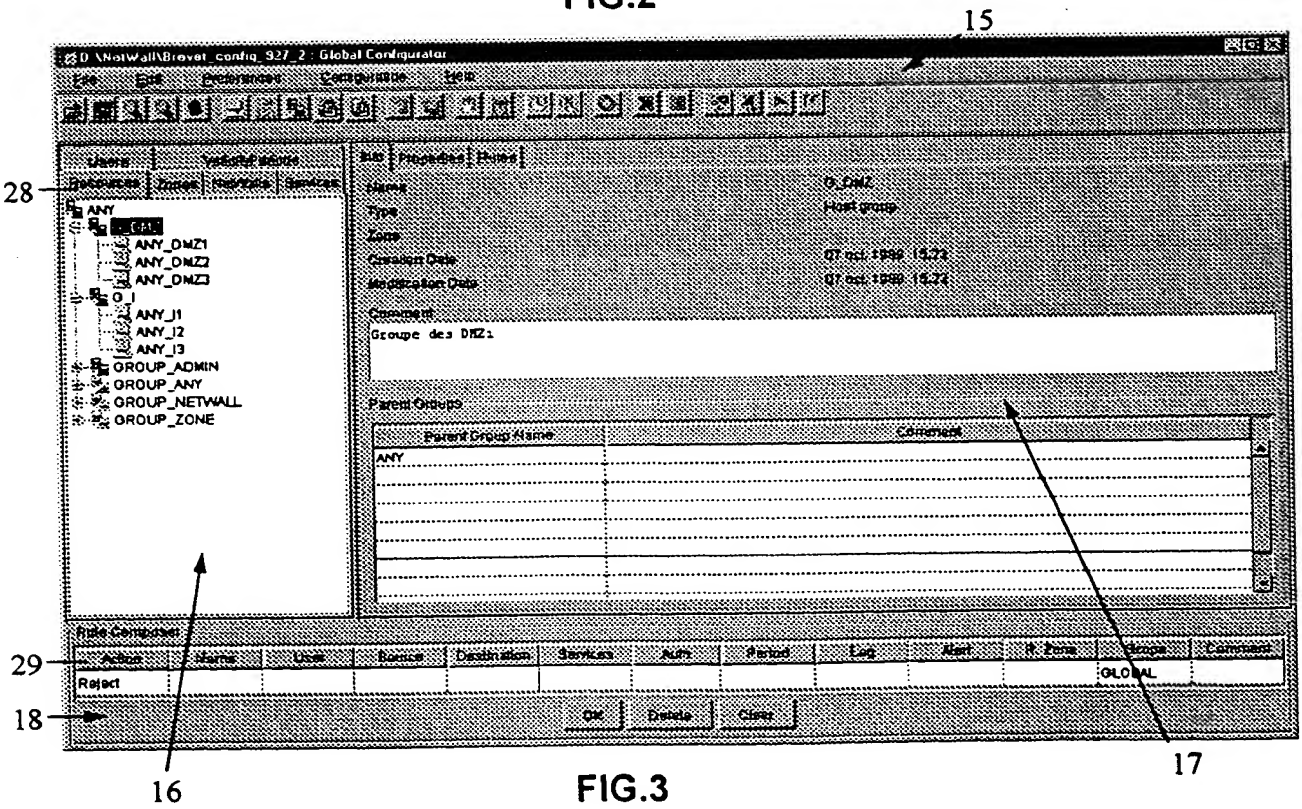
15
28
ANY
ANY_DMZ1
ANY_DMZ2
ANY_DMZ3
ANY_I1
ANY_I2
ANY_I3
GROUP_ADMIN
GROUP_ANY
GROUP_NETWALL
GROUP_ZONE
Parent Groups
Parent Group Name
Comment
ANY
29
Reject
GLOBAL
18
16
17

FIG.3

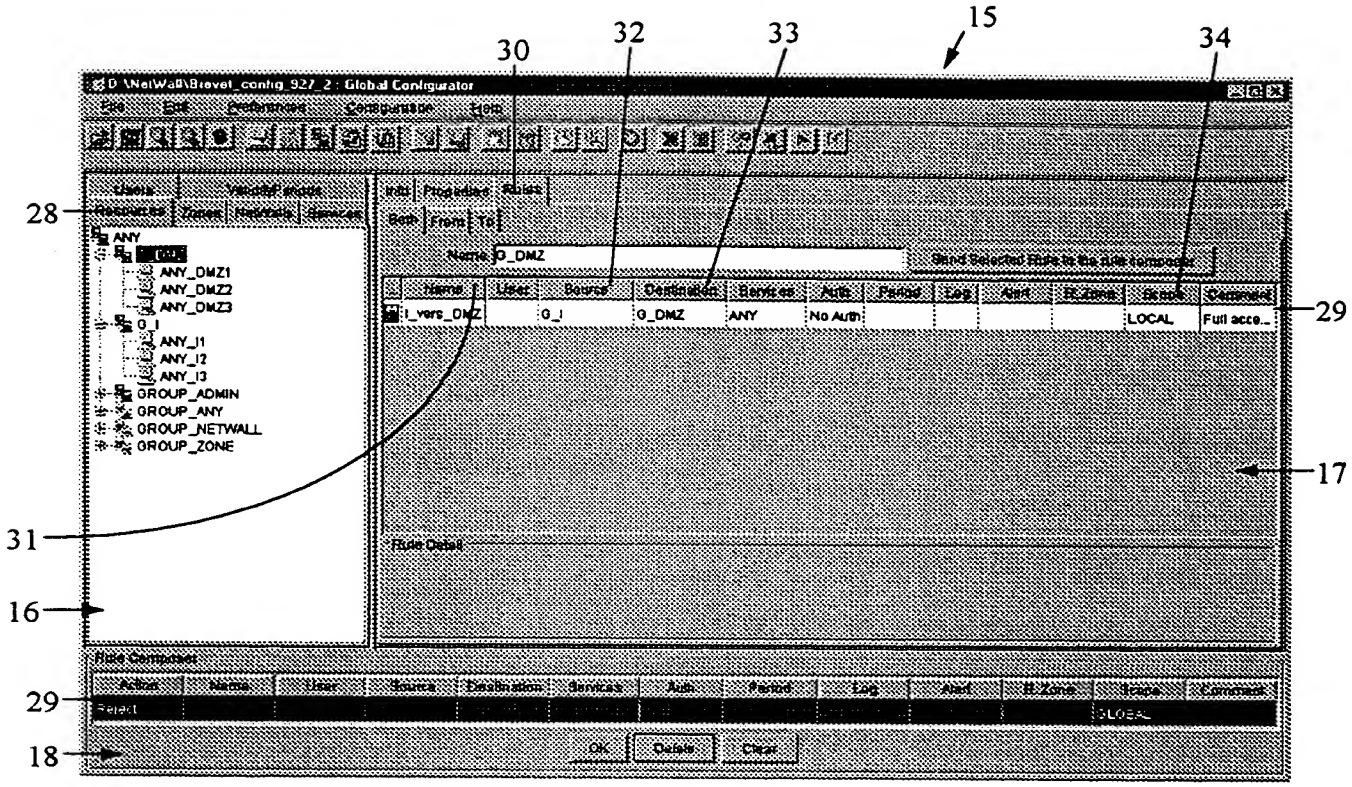
15
30
32
33
34
28
29
31
17
16
29
18
ANY
ANY_DMZ1
ANY_DMZ2
ANY_DMZ3
ANY_I1
ANY_I2
ANY_I3
GROUP_ADMIN
GROUP_ANY
GROUP_NETWALL
GROUP_ZONE
LOCAL
Full acce...
ANY
No Auth
Rule Detail
Rule Composer
OK
Delete
Clear

FIG.4